



# San Francisco Department of Public Health

## Policy Title: User Agreement for Confidentiality, Data Security, and Electronic Signature

Page 1 of 1

### SCOPE

The following applies to confidential, restricted, or protected SFDPH information and assets that are accessed, received or sent in any format, including digital, paper, voice, facsimile, photos, electronic signatures, etc.

### BACKGROUND

Individuals with access to SFDPH confidential information and data systems have a legal and ethical responsibility to protect the security and confidentiality of personal, medical, financial, personnel and protected health information, and to use that information and those systems only in the performance of their jobs.

The San Francisco Department of Public Health maintains electronic client records that support registration, clinical assessments, treatment plans, progress notes, medication management, client referrals, care authorization, provider payment activities, and billing. Federal law defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Under California law, a digital signature is defined as "an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature." "The purpose of a rendering/treating/ordering practitioner's signature in patients' medical records, operative reports, orders, test findings, etc., is to demonstrate the services have been accurately and fully documented, reviewed and authenticated. Furthermore, it confirms the provider has certified the medical necessity and reasonableness for the service(s) submitted to the Medicare program for payment consideration." For the purposes of this policy, an electronically signed record is a financial, program, or medical record that (1) is required to be signed under California or Federal law, California or Federal regulation, or organizational policy or procedure, and (2) may be requested during an audit.

### POLICY

Each staff will have a unique electronic signature that contains a title and/or a professional suffix that will be affixed to all electronically signed documents.

Every individual (USER) who is provided access to DPH patient or client information will signify ([User Agreement for Confidentiality, Security and Electronic Signature](#)) that they understand and agree to the terms and conditions outlined on the form.

Finally, users will attest that they understand that looking at patient information without having a business purpose is against the law and that violation of any of the requirements set forth in this User Agreement may result in termination of their employment, reporting to regulatory bodies, and reporting to their professional board.

Minimally, this form will be signed by users at time of hire, each time authorization to access a SFDPH data system is given, and annually thereafter. Signed forms are to be retained a minimum of 3 years post de-provisioning the individual's access to a SFDPH data system and/or termination of employment.